数理解析研究所講究録
第84巻 1970年 197-229

代数体における加法数論，特に Waring 問題について

金沢大理．江田義計

§1. Waring 問題．

Waring は彼の書物 Meditationes Algebraicae の第3版(1782)の中に[1]，すべての自然数は高々4個の平方数の和として，高々9個の立方数の和として，高々19個の4乗数の和として，等と表されると述べている。今自然数 $k \geqq 2$ を与えたとき，すべての自然数 n が高々 m 個の k-巾数の和として常に表わされるとすれば，m より大きい数については勿論この性質をもつが，このような m が存在すれば（それは k に関係するであろうが）その最小値を $g(k)$ で表わすことにする．本当に $g(2)=4$ を Liouville が，$g(3) \leqq 9$ は Wieferich が証明した(1909)．所が $23 = 2\cdot 2^3 + 7\cdot 1^3$，$239 = 2\cdot 4^3 + 4\cdot 3^3 + 3\cdot 1^3$ であって，この二数の立方数の個数はこれ以上へらすことが出来ないので $g(3)=9$ が確定する．しかし Landau は 1909 年に実は9個の立方数が必要であるものは有限個しかないと

いう驚くべき結果を与えた（後年1939年Dicksonは23と239以外にそのような数が存在しないことを示した）。さてHardyはvon SterneckやRuckleの計算した百万までの整数についての表を手にしていたが，8個を要するものは15個，7個の3乗和の必要な数は96しかなかった．Landauの定理によれば上記のWaringの問題では$g(k)$というのは問題の核心をついてはいないと言える．Landauの8もWieferichの9も大変深い意味をもつものではあるが。ここでHardyによって$g(k)$の代りに，より基本的な$G(k)$を定義しよう：整数のある所から先では常にM個又はそれ以下のk一乗和として表わされるようなMの最小値を$G(k)$とする．勿論$g(k)$の存在(a)から$G(k)$の存在(A)は直ちに分り$g(k) \geqq G(k)$は明かであるが(A)から逆に(a)の出ることも明かであろう。$g(2)=G(2)$である．Landauの定理から$G(3) \leqq 8$であるが$G(3) \leqq 7$はLinnik (1943)により，$G(4)=16$ (Davenport, 1939)があるが一般に($g(k)$や) $G(k)$を決定することは非常に面倒である．$g(k)$に関しては1940年頃までにはDicksonやPillaiによって$k=4, 5$を除いて決定された．最近(1964) J.R. Chenによって$g(5)=37$が報ぜられているので，幸に$g(k)$については$19 \leqq g(4) \leqq 35$ (Dickson, 1933)だけが未解決のようである．

Hilbertは1909年に$g(k)$の(従って$G(k)$の)存在を半ば解

析学的に半ば算術的に証明した[2] 彼が用いた積分法を取り去り全く初等的に証明するなどの改良が加えられては来たが $g(k)$ の決定は簡単な場合でも出来なかった。

かくて我々に与えられる問題としては $G(k)$ の決定，または $G(k)$ の上界を求めることが重要となる．$G(k) \geq k+1$ はすぐ分るのである．我々がこれから Waring 問題というのは上記の問題であるとする．Waring 問題の理解の為には [3]～[8] をあげておく．[9], [10] は必読の書であろう（[6], [9], [10] は雑誌数学に書評がある）．Waring 問題とその周辺の問題との事情については [11]～[13] をあげる．[14], [15] は論文集であるが，これらによって大いに勇気づけられ度い．後記の文献は我々の目的に必要なもののみに限ることにした．無数にある(?)論文はいつかどこかでまとめられることを期待したい。

§2. Hardy-Littlewood の円周法． Hilbert の定理によれば Waring の提出した問題の半ば（その存在）は解決され，また後には $g(k)$ の決定まで与えられているのであるが，単に $g(k)$ の存在というのでなく，更に広い視野のもとに，この種の問題に強力な武器を与えたのが Hardy-Littlewood による circle-method と呼ばれるものである．Waring 問題については彼等は終始共著として論文を出しているので今後二人を H-L と

略記することにする．彼等の考え方，成功するまでの苦心などは Hardy 自身の語る所にくわしい [12]．この方法では $G(k)$ の上界だけでなく k 巾和としての表わし方の個数の評価をも同時に与える：

今整数論的函数 $r(n)$ とその生成函数を $F(x)=\sum_{n=0}^{\infty} r(n)x^n$ とするとき Cauchy の定理から

$$r(n) = \frac{1}{2\pi i}\int \frac{F(x)}{x^{n+1}}\,dx$$

として $r(n)$ を与えることにする．$F(x)$ は単位円で regular で積分は円周 $|x| = r < 1$ に沿うものとする．Waring 問題の場合には

$$f(x) = 1 + 2\sum_{n=1}^{\infty} x^{n^k}$$

として

$$F(x) = (f(x))^s = \sum_{n=0}^{\infty} r_{k.s}(n)\,x^n$$

を上の公式に代入して積分するのである．ここで $r_{k.s}(n)$ は n を整数の k-巾の（絶対値の）和として表わす仕方の個数である．k が偶数ならもちろん k 巾和表示の個数に等しい．

(1) $$r(n) = r_{k.s}(n) = \frac{1}{2\pi i}\int\left\{(f(x))^s/x^{n+1}\right\}dx$$

を得る．積分は $|x| = e^{-1/n}$ に沿うのである．つまりこの時 x は $x = e^{-1/n + 2\pi i\theta}$ とかける．有理数 $\theta = p/q$ において，$1 \leq q \leq n^{1-1/k}$，$(p, q) = 1$，$0 \leq p < q$ であれば $n^{1-\frac{1}{k}}$ 次の Farey 分数であるという．$0 = 0/1$，$1 = 1/1$ として共に Farey

分数の中間に入れる。二つの Farey 分数 $\theta = p/q$, $\theta' = p'/q'$ が隣り合っていればそれ等の中間値によって円周(又は長さ 1 の線分)を切断すると各 Farey 分数にはそれぞれ一つの円弧(又は線分) $M_\theta = M_{p.q}$ が与えられる。この時特に Farey 分数 $\theta = p/q$ で $q \leq n^{1/k}$ をもつものを(対応する線分を) major arcs と呼び、それ以外のもの従って $n^{\frac{1}{k}} < q \leq n^{1-\frac{1}{k}}$ を分数にもつ区間を minor arcs と呼ぶことにする。後者の場合は $m_{p.q}$ で区間を表わし、その区間の総和を $\sum m_{p.q} = \mathfrak{E}$ で表示することにしよう。かくて積分(1)は次の二つに分れる:

$$r_{k.s}(n) = \sum_{\theta} \frac{1}{2\pi i}\int_{M_\theta} \cdots\cdots + \frac{1}{2\pi i}\int_{\mathfrak{E}} \cdots\cdots$$

実は Farey 分割(上の意味)を生成函数と共に、H-L が Waring 問題を取扱った 1920 年より少し前に、すでに Hardy は Ramanujan との共著の [16] で用いていた。そこでは生成函数はダ円モヂュラー函数であった。

さて上記二つの積分の取扱ひであるが、Major arcs では $(f(x))^s$ の代りに

$$(2)\quad \begin{cases} F_{p.q} = C\,\Gamma\left(\frac{s}{k}\right)\left(\dfrac{S_{p.q}}{q}\right)^s \left(\log\left(\dfrac{e^{2\pi i\, p/q}}{x}\right)\right)^{-s/k} \\ C = \left(2\Gamma\left(1+\frac{1}{k}\right)\right)^s \Big/ \Gamma(s/k) \\ S_{p.q} = \sum_{h=0}^{q-1} e^{2\pi i\, h^k p/q} \end{cases}$$

を用いた。このような代用が最後まで破綻なく実行された理だが、([12] 参照) 丁度 1916 年に Weyl によって出されていた

名著[17]の中の三角和の評価が有効に働いた．（三角和とは指数函数の（有限個の）和）．minor arc $\mathcal{E}$ の取扱いもWeylの不等式とも呼ばれる上述の方法がうまく利用された．彼等が得た結果[19]では，$s > k2^{k-1}$ のとき $(n \to \infty)$

$$(3) \qquad r(n) \sim C \cdot \sigma \cdot n^{-1+\frac{s}{k}}$$

ここで

$$(4) \qquad \sigma = \sum_{q=1}^{\infty} \frac{1}{q^s} \sum_{\substack{p=1 \\ (p\cdot q)=1}}^{q} \left(S_{p\cdot q} \right)^s e^{-2\pi i n \frac{p}{q}}$$

であった．この σ のことをsingular seriesと呼んだ．最初の[18]では n のすべての値に対して $k=4$, $s=33$ だけ，[19]では $k \geqq 3$ で上記のとき σ が|Conv|（絶対収束）してある正数 c_1, c_2 に対して

$$(5) \qquad 0 < c_1 < \sigma < c_2$$

が言えた．H-Lは其の後もPartitio Numerorum II (1921) [20], IV (1922) [21], VI (1925) [22] そして VIII (1928) [23] とそれぞれ興味ある結果を与えているのであるが[14]，P. N. VI によって一つの注意をしておく：

任意の $\varepsilon > 0$ に対して不定方程式

$$(6) \qquad n = x_1^k + \cdots + x_k^k$$

の解の個数がもし $O(n^{\varepsilon})$ しかないならば（この仮定をKとする）(7) $\quad s \geqq 2k+1$

で(3)が成立することを示した．$k=3$ ではK. Mahlerが不

成立を示したが(1936), $k \geq 4$ では未だ未解決である.

Hardy-Littlewood 以後. 重大な改良を与えたのは I. M. Vinogradov である. [24]～[27]. それは巾級数と Cauchy の定理の代りに三角和の積分でおきかえ, 三角和の評価をもって(3)を与えようとするものである. H-L の方法に長くを費したし, 我々の目的である代数体での取扱いは Vinogradov の方法によるものなので, 彼の所論とテクニクは Siegel の方法によって知っていただきたい. 更には今は彼の名著も英訳されている[9], [8], [10] のあることも前述の通りである.

彼の得た結果のいくつかを後§の為にあげておく:

(8) $G(k) \leq 6k\log k + (\log 216 + 4)k$ (1934) [25]

(9) $G(k) \leq 3k\log k + 11k$ (1954) [9]

そして最近 (Vinogradov, I.M. は 1891年生れ) 更に改良して

(10) $G(k) \leq 2k\log k + 4k\log\log k + 2k\log\log\log k + 13k$ $(k \geq C)$ (1959) [27]

とした.

(10) は (7) と比較すると, この方法での final stage とも見られそうである.

§3. Vinogradov-Siegel の理論.

1900年パリでの Hilbert の講演にある未解決の問題が直接の

事情かも知れないが Landau, Meißner, Artin と続いて代数体での加法数論が論ぜられて来たが, Siegel も 1920 年[28]頃から加法数論に手をつけている. H-L の Waring 問題が出て間もなく, 早速彼等の円周法を代数体で実行することを試みている [29], [30]. ここでは直ちに彼が Hardy Littlewood として Vinogradov の方法によって代数体での Waring 問題の解決した所を紹介することとしよう. [31], [32] (前者では totally real の場合, 後者では虚の共役のある場合を論じている). [29], [30] から [31], [32] を得るまでには Siegel をもってしても十数年を要したのである. 1945 年の彼の [31] から彼の言葉に少し耳を傾けよう: The generalization of the major and minor arcs of the Farey dissection led to a difficulty which I could not overcome at that time. Recently I found the solution. 以下では Vinogradov の [9] を参考として Siegel の方法と結果とを, 特に代数体での Farey 分割の方法をのべる.

先ず彼による注意を: J_k を K の整数環 $\mathfrak{O}$ の中で $\mathfrak{O}$ の元の k 乗で生成される加法群とする. $[\mathfrak{O}:J_k]$ は有限だが必ずしも $\mathfrak{O}=J_k$ とならないことを Siegel が注意した. 彼の例をあげると判別式 $=4d$ ($d\equiv 2, 3 \pmod 4$) をもつ実二次体では $p+q\sqrt{d}$ ($2\nmid q$, $p, q\in\mathbb{Z}$) は平方和にならない! 従って以下では等巾和問題を考えるときは J_k の中で考察するのである.

まづ最後まで必要な記号をあげる：代数体 $K \ni \gamma$ のとき n_1 個の実共役体 $K^{(l)} \ni \gamma^{(l)}$，$2n_2$ 個の虚共役体 $K^{(m)}, K^{(m+n_2)} \ni \gamma^{(m)}, \gamma^{(m+n_2)}$ とし之れ等は複素共役数とする．$\xi = \sum_{i=1}^{n} \gamma_i x_i$ $(\gamma_i \in K)$ に対して $\xi^{(j)} = \sum_{i=1}^{n} \gamma_i^{(j)} x_i$ $(1 \leq j \leq n)$，$n = n_1 + 2n_2$,
(x_i：実変数)

$\mathrm{trace}\,\xi = \sum_{j=1}^{n} \xi^{(j)}, = tr(\xi)$. $\|\gamma\| = \mathrm{Max}_i |\gamma^{(i)}|$

$E(\xi) = e^{2\pi i\, tr(\xi)}$. $K \ni \gamma$ が totally positive (non negative) とは $\gamma^{(l)} > 0$ $(1 \leq l \leq n_1)$, $(\gamma^{(l)} \geq 0\ (1 \leq l \leq n_1))$ 更に $|\gamma^{(i)}| \leq \Gamma$ $(1 \leq i \leq n)$ の条件があれば $\gamma < \Gamma$ と記す．

ϑ は K の共役差積で $\vartheta^{-1} = \{\rho : E(\alpha\rho) = 1 \quad \forall \alpha \in \mathfrak{O}\}$．$\gamma\vartheta = \mathfrak{b}/\mathfrak{a}$ $(\mathfrak{a}, \mathfrak{b}) = 1$，$\mathfrak{a}, \mathfrak{b}$ 整イデアル，このとき $\gamma \longrightarrow \mathfrak{a}$ で表わす．

$\gamma \longrightarrow \mathfrak{a}$，$\lambda, \mu \in \mathfrak{O}$，$\lambda \equiv \mu \pmod{\mathfrak{a}}$ なら $E(\lambda^k \gamma) = E(\mu^k \gamma)$ 等を得る．$\mathfrak{O}$ と ϑ^{-1} の基表示 $[\omega_1, \cdots, \omega_n]$, $[\rho_1, \cdots, \rho_n]$ の間では $tr(\rho_r \omega_s) = \delta_{rs}$ (Kronecker の Δ) に取れる．T は十分大として

(11) $\qquad t = T^{1-a}, \quad h = T^{k+a-1} \qquad (0 < a < 1) \quad (T^{2n} > 2D^{1/n})$

Siegel は $a = 1/(2^{k-1} + n)$ に取った．これについては後述．

単位立方 $U = \{(x_1, \cdots, x_n), 0 \leq x_i \leq 1, (1 \leq i \leq n)\}$；$U \ni (x_1, \cdots, x_n)$ をもって $\gamma = \rho_1 x_1 + \cdots + \rho_n x_n$ を作る．$x_1 \cdots x_n$ が有理数のとき $\gamma \longrightarrow \mathfrak{a}$，$N\mathfrak{a} \leq t^n$ である γ の集合を Γ で表わす．$\xi = \rho_1 x_1 + \cdots + \rho_n x_n$，$\eta = \omega_1 y_1 + \cdots + \omega_n y_n$ のとき $dx_1 \cdots dx_n = dx$, $dy_1 \cdots dy_n = dy$ 等と記す．さて Farey 分割に対する major arc を

Siegel によって定義すると，$\Gamma \ni \gamma$ に対し（そして h, t に関して）

(12) $M_\gamma = \{ (x_1, \ldots, x_n)\ ;\ (x_1, \ldots, x_n) \in U,$

$$\prod_{i=1}^{n} \mathrm{Max}\,(h |\xi^{(i)} - \gamma^{(i)}|,\ 1/t) \leq 1/Nn\ , \text{ for any } \gamma_0 \equiv \gamma\ (\vartheta^{-1}) \}$$

このとき $M_\gamma \ni \xi$ と略記する．$\gamma \neq \gamma'$ なら $M_\gamma \cap M_{\gamma'} =$ 空集合である．$E - \bigcup_\gamma M_\gamma = \mathcal{E}(h, t) = \mathcal{E}$ を minor arc と呼ぶ．

$\mathcal{E}(h, t) \ni \xi$ に対して Siegel の得た次の結果は有理数体では至極簡単なことではあるが以後の計算に対して重要で決定的な役目を果して呉れる．

定理 1．$\mathcal{E}(h, t) \ni \xi$ に対して

1) $\alpha \in \mathfrak{O}$，$\beta \in \vartheta^{-1}$ が存在して

2) $|\alpha^{(i)}\xi^{(i)} - \beta^{(i)}| < h^{-1}$，$0 < |\alpha^{(i)}| \leq h$ $\quad (1 \leq i \leq n)$

3) $\mathrm{Max}\,(|\alpha^{(1)}|, \ldots, |\alpha^{(n)}|) = \|\alpha\| > t$，

4) $\mathrm{Max}\,(h|\alpha^{(i)}\xi^{(i)} - \beta^{(i)}|, |\alpha^{(i)}|) \geq D^{-1/2}$ $\quad (1 \leq i \leq n)$

5) $N((\alpha, \beta\vartheta)) \leq D^{1/2}$．

証明はあとで述べるとして Siegel の得た結果の一つを記す

定理 2．$n_2 > 0$ とし $0 < \lambda^{(l)} < T$ $(1 \leq l \leq n_1)$，$|\lambda^{(m)}| \leq T$ $(n_1 + 1 \leq m \leq n$，$\lambda \in \mathfrak{O}$ である範囲を $\Omega(T)$ で表わす．（$\lambda < T$ と記した）．

(13) $$f(\lambda) = \sum_{\lambda \in \Omega(T)} E(\lambda^k \xi)\ ,$$

(14) $s \geq (2^{k-1} + n)kn + 1$

(15) $$A_s(\nu) = \int_U (f(\lambda))^s E(-\nu\xi)\, dx$$

とおくと

(16) $$A_s(\nu) = J \cdot \sigma \cdot T^{n(s-k)} + o\left(T^{n(s-k)}\right)$$

を得る。これは H-L の K での結果であり，Hilbert の定理の拡張でもある。ここで σ は Singular series であって

(17) $$\sigma = \sigma(\nu) = \sum_{\mathfrak{a}} H(\mathfrak{a}) \qquad |\mathrm{conv}|$$

$$H(\mathfrak{a}) = \sum_{\substack{\gamma \\ \gamma \to \mathfrak{a}}} \left(\frac{S(\gamma)}{N\mathfrak{a}}\right)^s E(-\nu\gamma) \qquad \nu \in \mathfrak{G}$$

（ここで γ は $1/\mathfrak{a}\mathfrak{d}$ 内の mod $1/\mathfrak{d}$ の reduced residue system を動く）

(18) $$S(\gamma) = \sum_{\lambda \bmod \mathfrak{a}} E(\lambda^k \gamma),$$

であるが s が (14) の条件をもつときに $\nu \in J_k$ なら c_1, c_2 なる定数があって

(19) $$c_1 > \sigma > c_2 > 0$$

を得る。もし $\nu \notin J_k$ であったら前の注意（p.8，下）のように $\sigma = 0$。更に J は $\mu < 1$ なる μ できまるもので $s > k+1$ のとき

(19) $$J = J(\mu) = \int_X \Phi_1(\xi) E(-\mu\xi)\,dx, \quad \Phi_1(\xi) = \left(\int_{\eta<1} E(\eta^k \xi)\,dy\right)^s$$

$$= D^{\frac{1}{2}(1-s)} \prod_{l=1}^{n_1+n_2-1} F(\mu^{(l)}) \prod_{m=n_1+1}^{n_1+n_2} H(\mu^{(m)}) > 0$$

$$F(\mu^{(l)}) = \frac{\Gamma^s(1+1/k)}{\Gamma(s/k)} (\mu^{(l)})^{\frac{s}{k}-1}$$

$$H(\mu^{(m)}) = k^{-1} \int_{\mathfrak{D}} \sum_{r=1}^{s} \left(k^{-1} u_r^{\frac{1}{k}-1}\right) du_1 \cdots du_{s-1}\, d\varphi_1 \cdots d\varphi_{s-1}$$

$$\mathfrak{D}: 0 < u_r < 1 \ (1 \le r \le s), \quad -\pi < \varphi_r < \pi \ (1 \le r \le s-1)$$

$$u_s = \left|\mu^{(m)} - (u_1^{1/2} e^{i\varphi_1} + \cdots + u_{s-1}^{1/2} e^{i\varphi_{s-1}})\right|^2$$

なお最後の追記の定理 2′ を見よ。

Siegel は [31] では totally real の場合を取扱っているが，それは H-L の (3) と比較しても分りよいであろう：$A(\nu)$ の形は

$$(20)\qquad A(\nu) = D^{\frac{1}{2}(1-s)}\ \frac{\Gamma^{s}(1+1/k)}{\Gamma(s/k)}\ \sigma\ N(\nu)^{\frac{s}{k}-1} + o\left(N(\nu)^{\frac{s}{k}-1}\right)$$

ここでは

$A(\nu)$ は $\lambda_1^{k}+\cdots+\lambda_s^{k}=\nu$ の totally positive な解 $(\lambda_1,\cdots,\lambda_s)$ の解の個数である．(16)〜(20) に対してはこれ以上触れないが，(13) の中の積分で置き換えたのは Vinogradov である．ここで定理 1 の証明を与えておく [32].

1) と 2)：連立不等式

$$\begin{cases} |x_1\omega_1^{(i)}+\cdots+x_n\omega_n^{(i)}| \leq h \\ |x_1\xi^{(i)}\omega_1^{(i)}+\cdots+x_n\xi^{(i)}\omega_n^{(i)} - z_1\rho_1^{(i)}-\cdots-z_n\rho_n^{(i)}| < h^{-1} \end{cases} \qquad (1\leq i\leq n)$$

に Minkowski の定理を用いると有理数 $x_1,\cdots,x_n$, $z_1,\cdots,z_n$ があって $\alpha=\omega_1x_1+\cdots+\omega_nx_n$, $\beta=z_1\rho_1+\cdots+z_n\rho_n$ とおくと $\alpha\in\mathfrak{o}$, $\beta\in\vartheta^{-1}$ であって明かに $|\alpha^{(i)}\xi^{(i)}-\beta^{(i)}|<h^{-1}$ $0\leq|\alpha^{(i)}|\leq h$ $(1\leq i\leq n)$ を得るが．もし $\alpha=0$ なら $|\beta^{(i)}|<\frac{1}{h}$ $(1\leq i\leq n)$ だから $|N\beta|<h^{-n}\leq D^{-1}$ となり T が十分大なら $\beta\in\vartheta^{-1}$ に反する．だから $\alpha\neq0$ それが 2)．

3) $\mathcal{E}(h,x)\ni\xi=\rho_1y_1+\cdots+\rho_ny_n$ であるから，今 $\beta/\alpha=\rho\to\mathfrak{a}$ とおくと（このとき $\mathfrak{a}|\alpha$）$N\mathfrak{a}\leq T^n$ ならば

$$\prod_{i=1}^{n}\mathrm{Max}\left(h|\xi^{(i)}-\rho^{(i)}|,\ T^{-1}\right) > N(\mathfrak{a})^{-1}$$

（$N\mathfrak{a}>T^n$ ならこの式は明か）$\therefore |N(\alpha)|\geq N\mathfrak{a}$ 従って

$$\prod_{i=1}^{n} \mathrm{Max}\,(\,t|\alpha^{(i)}\xi^{(i)}-\beta^{(i)}|,\ |\alpha^{(i)}|T^{-1}) > 1$$

故にある i で $|\alpha^{(i)}|T > 1$ つまり $\|\alpha\| > T$.

4) (α, β) の対で 1), 2) を満足するものの集合を S とおく. $|\alpha^{(r)}| \geqq D^{-1/2}$ ならすでに言うことなし. $|\alpha^{(r)}| < D^{-1/2}$ のときは $t|\alpha^{(r)}\xi^{(r)}-\beta^{(r)}| \geqq D^{-1/2}$ であることが言われればそれでよい. $(\alpha, \beta\vartheta) = \mathfrak{q}^{-1}$ とおく $N\mathfrak{q} \leqq 1$, $N\mathfrak{q}D^{1/2} \leqq D^{1/2}$ を得る. ここで r が $1 \leqq r \leqq n_1$ なら $0 < |x^{(r)}| \leqq D^{1/2}$, $|x^{(i)}| < 1$ $(i \neq r)$ もし r が $n_1+1 \leqq r \leqq n_1+n_2$ であれば $0 < |x^{(r)}| \leqq D^{1/4}$, $|x^{(i)}| < 1$ $(i \neq r, r+n_2)$ として, Minkowski の定理を用いると $\mathfrak{q} \ni x$ で $0 < |x^{(r)}| \leqq D^{1/2}$, $|x^{(i)}| < 1$ $(i \neq r)$ なるものあり $x\alpha = \hat{\alpha}$, $x\beta = \hat{\beta}$ とおくと $|\hat{\alpha}^{(r)}| < |\alpha^{(r)}|$ を得る. そこで S の中に (α, β) で $\mathrm{Min}\,\|\alpha\| = b \geqq 1$ をもつものを (α_0, β_0) とおく. これに対し上と同じ操作で $(\hat{\alpha}_0, \hat{\beta}_0)$ を作ると $b \leqq \|\hat{\alpha}_0\| < \mathrm{Max}\,(\|\alpha_0\|) = b$ となり矛盾. だから

$$|x^{(i)}(\alpha^{(i)}\xi^{(i)}-\beta^{(i)})| < t^{-1}, \quad |x^{(i)}||\alpha^{(i)}| \leqq t \quad (1 \leqq i \leqq n)$$

ではない筈であるが $|x^{(i)}||\alpha^{(i)}| \leqq t$ $(1 \leqq i \leqq n)$ は常に成立しているし $|x^{(i)}||\alpha^{(i)}\xi^{(i)}-\beta^{(i)}| < t^{-1}$ $(i \neq r)$ も成立している残る所は $i = r$ の時不成立の筈で

$$|\alpha^{(r)}\xi^{(r)}-\beta^{(r)}| \geqq t^{-1}\,|x^{(r)}|^{-1}.$$

$$\therefore\ t|\alpha^{(r)}\xi^{(r)}-\beta^{(r)}| \geqq |x^{(r)}|^{-1} \geqq D^{-1/2}$$

5) 4) のように $\|\alpha\| = b$ が最小値とする 3) から $b > T$,

$\mathfrak{q} = (\alpha, \beta\vartheta)^{-1} \ni x$ を取ると $x\alpha = \hat{\alpha} \in \mathfrak{O}$, $x\beta = \hat{\beta} \in \vartheta^{-1}$ になる. $N\mathfrak{q} \geqq D^{-1/2}$ ならそれでよいが $N\mathfrak{q} < D^{-\frac{1}{2}}$ であれば再び Minkowski の定理から $|x^{(1)}|, \dots, |x^{(n)}| < 1$ に取れて $(\hat{\alpha}, \hat{\beta})$ が S に入ったとき矛盾は出るが, それは前述の通り, だから 5).

§4 Siegel 以後

§3 の Siegel の定理のあと十数年たって (1958年[33]) Tatuzawa は Vinogradov の本 [9] の結果を発展させて Siegel を非常によく

(21) $$G_K(k) < 8n\, k(n+k)$$

とした. 証明には次の定理 3, 定理 4 が重要な役目をする. 勿論 Weyl の三角和の評価の代数体での取扱いの Siegel の方法も用いている ($G_K(k)$ は K での $G(k)$ に対応するもの).

定理 3. $\lambda_1, \dots, \lambda_s$ を $\mathfrak{O}$ の元を独立に mod $\mathfrak{a}$ の完全剰余系を動かすとき, ν を与えて ($\in \mathfrak{O}$)

$$\lambda_1^k + \cdots + \lambda_s^k \equiv \nu \pmod{\mathfrak{a}} \quad (\nu \in J_k)$$

の解の個数を $M(\nu, \mathfrak{a}) = M(\mathfrak{a})$ とおくと (合同 Waring 問題!)

$$M(\mathfrak{a}) = N(\mathfrak{a})^{s-1} \sum_{\mathfrak{f} | \mathfrak{a}} H(\mathfrak{f})$$

を得るのであるが, $\mathfrak{p}$ を K の素イデアルとし $\mathfrak{a} = \mathfrak{p}^l$ の場合を考察するに, $N\mathfrak{p} = p^f$ (p は素数), $\mathfrak{p}^e \| p$, $p^b \| k$ ($k \geqq 3$), $l_0 = (b+2)e$, $s_0 = [8nk(\log k + 1)]$, でもし $l \geqq l_0$, $s \geqq s_0$, のとき

$$M(\nu, \mathfrak{p}^l) \geqq N(\mathfrak{p})^{(l - l_0)(s-1)}$$

である．($a^e \| b$ は $a^e | b$, $a^{e+1} \nmid b$ のこと)．

これは Waring 問題に大切で，これから $k \geq 3$, $s \geq s_0$, $\nu \in J_k$ のとき $\sigma = \sigma(\nu) = \sum_{\mathfrak{a}} H(\mathfrak{a})$ |Conv| が出て $\sigma(\nu) > c_0 > 0$ が出る，更に $\chi(\mathfrak{p}) = \sum_{l=0}^{\infty} H(\mathfrak{p}^l)$ も |Conv| で積公式

$$\sigma(\nu) = \prod_{\mathfrak{p}} \chi(\mathfrak{p})$$

を得るのである．もう一つ大切な定理：

定理4. $\sigma_i < T$, $(1 \leq i \leq s)$ によって $\mu = \sigma_1^k + \cdots + \sigma_s^k$ と表わされる μ の集合を $\mathfrak{Q}_{\mathfrak{o}}(s, T)$ としその個数を $\#(\mathfrak{Q}_{\mathfrak{o}}(s,T))$ で表わすと

$$\#(\mathfrak{Q}_{\mathfrak{o}}(s,T)) \geq c\, T^{nk\{1-(1-\frac{1}{k})^l\}}, \quad l = [s/n]$$

である．

Tatuzawa [33] の翌年 Mitani によって代数体に於ける Goldbach 問題が出た，[64] これは Vinogradov の有理数体での定理の代数体での見事な結果であった，その中の一つの定理をあげる．

定理5. K で $\mathfrak{a}_0$ を固定したイデアル，$\mathfrak{c}$ を任意のイデアル，$\mathfrak{a}_0\mathfrak{c}$ の底を $[\eta_1, \dots, \eta_n]$ としそれぞれ $|\eta_j^{(i)}| \leq c\, N(\mathfrak{a}_0\mathfrak{c})^{1/n}$ $(1 \leq i, j \leq n)$ とする．(下側の不等式も取れる．このように取った η_i を正規化されたということにする．) n-次元ユークリッド空間 E^n の平行六面体 $M = \{(x_1, \dots, x_n),\ a_j \leq x_j \leq b_j\ (1 \leq j \leq n)\}$ とし，$\varepsilon = \varepsilon(h,t) \ni \xi$, $V = \mathrm{Max}(1, b_1 - a_1, \dots, b_n - a_n) < h/(2^{3+n_2}(DN(\mathfrak{a}_0\mathfrak{c}))^{1/n})$

とし

$$Z = \sum_{\substack{\mu \in \mathfrak{a}_0^{-1} \\ x(\xi) \in M}} \mathop{\mathrm{Min}}_{1 \leq j \leq n} (u, \langle S(\eta_j \mu \xi) \rangle^{-1}) \quad (u \geq 1) \quad (h > 2Dt,\ t > 1)$$

ならば

$$Z \ll V^n U N(C)\left(\frac{1}{t}+\frac{1}{V}+\frac{h\log h}{VUN(C)^{1/n}}+\frac{\log h}{U}\right)$$ である.

Tatuzawa は [33] の Supplement [36] で 定理5を使えば (21) が更に改良されることを注意し，また先生の未刊の原稿 [37] で次の結果の証明を与えている.

(22) $$G_K(k) \leq \mathrm{Min}\left(4nk\left[\frac{\log(4k)}{\log 2}\right],\ 2^k+1\right) \qquad (1962)$$

また

(23) $$G_K(k) \leqq 4nk\left[\frac{\log(4k)}{\log 2}\right] + 2n\,G(k) \qquad (1962)$$

ここで $G(k)$ には p.7 の (8)〜(80) が使える理である.

一方 Tatuzawa が出て間もなく Körner は更によくして

(24) $$G_K(k) < nk\left(3\log k + 3\log\left(\frac{n^2+1}{2}\right) + 11\right) \qquad (1961)$$

とした，これは Vinogradov の結果であり [9] の方法をより忠実に実行に移したものであった [38]. 彼は定理3で s_0 を $4nk$ とおくことが出来ることを示したのである. この場合を定理3′ としよう

なおこれについて Stemmer [39] 参照, $s_0 = ef(2k-1)\ (k \geq 3)$ としている. なおまた合同 Waring 問題や p-進体での等巾和問題についてはのべないが [34], [35] 参照.

§5 Vinogradov の平均値定理

§2 での Siegel の方法は Hardy-Littlewood そして Vinogradov Siegel の方法とも言うべきものであるが，実は Vinogradov の

1934～35年頃から発展して来た現在彼の名で呼ばれている平均値定理というものがあり，彼の1959年の結果(10)はそれを更によくしたものであった．これについてはHuaの本[10]，綜合報告[40]，[41]が明解である．さてその平均値定理とは，整数 $\nu_1,\dots,\nu_k$ を与えて連立不定方程式

$$
(25)\quad \begin{cases} \lambda_1+\cdots+\lambda_s=\mu_1+\cdots+\mu_s+\nu_1 \\ \lambda_1^2+\cdots+\lambda_s^2=\mu_1^2+\cdots+\mu_s^2+\nu_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \lambda_1^k+\cdots+\lambda_s^k=\mu_1^k+\cdots+\mu_s^k+\nu_k, \quad 0\le\lambda_i,\mu_i\le T,\ (1\le i\le s) \end{cases}
$$

の解の個数を $N_{k,s}(T;\nu_1,\dots,\nu_s)$ $\left(N_{k,s}(T,0\cdots0)=N_{k,s}(T)\right.$ とおく$\left.\right)$ を求める又は評価する問題である．これは

$$
(26)\quad L(\xi_k,\dots,\xi_1)=\sum_{0\le\lambda\le T} e^{2\pi i(\xi_k\lambda^k+\cdots+\xi_1\lambda)}
$$

とすると

$$
(27)\quad N_{s,k}(T,\nu_1\cdots\nu_s)=\int_0^1\cdots\int_0^1 |L(\xi_k,\dots,\xi_1)|^{2s} e^{2\pi i(\nu_1\xi_1+\cdots+\nu_k\xi_k)}\,d\xi_1\cdots d\xi_k
$$

によって与えられる．

$N_{s,k}(T)$ についてはHuaのすぐれた結果が1949年に与えられ[42]，その応用と共に[10]でくわしい．また応用についてはWalfiszの綜合報告[43]が新しい．(Waring以外の問題について)．更に最近(1963年) KaracubaとKorobovとはVinogradov-Huaとは着想の全く異なる非常に明解な勝れた研究であるが[44]，実はそれは代数体で考えた時に，より勝れたものであることが分る．

平均値定理の代数体での取扱いは 1959 年に Tatuzawa [45] によって totally real の場合に Hua の方法によって報告されているが，数年後には Körner [46] も矢張り Hua のやり方で一般の場合に求められ，Hua の発想による "一般なる Waring 問題" [47] つまり多項式 $f(x)$ を与えた時に ν を $f(\lambda_1)+\cdots+f(\lambda_s)$ として表はす問題に応用している．代数体でのこの問題は Ayoub [48] も Siegel 流に扱っている．　　では Eda [49] の結果をあげる：

定理 6　(25) で整数 $\lambda_i, \mu_i \in \mathfrak{O}$ はすべて $\lambda_i, \mu_i < T$ (T は十分大) とし体 K の拡大次数 $n \geq 2$, 自然数 $k \geq 2$, 自然数 $\tau \geq 1$ とする．このとき

$$s \geq \frac{1}{2}\frac{n}{(n-1)}k(k+1)+\tau k-1 \tag{28}$$

ならば (従って $s \geq k(k+1)+\tau k-1$ でよいが)

$$N_{s,k}(T) \leqq c^{\tau\left(k^2+2s+\frac{(\tau-1)}{k}s-\frac{1}{4}(\tau-1)(k+1)\right)}\cdot s^{2k\tau}\cdot T^{\left(2s-\frac{1}{2}k(k+1)+\frac{1}{2}k(k+1)\left(1-\frac{1}{k}\right)^{\tau}\right)n} \tag{29}$$

となる．ここで c は K のみによる定数である．(c は $n\to\infty$ では $c'>1$ として $c'^{\,n\log n}$ 位には大きくなりうるものである．)

証明は (26), (27) 等での $e^{2\pi i}$ は $E(\cdots)$ で置きかえられなければならぬことは勿論であるが，もはや記号や詳細は省くとしてごくごく簡単に方針だけのべてみよう：

$\nu = 1, \cdots \tau$ に対して，$\mathfrak{g}_j, P_j, \pi_j$ を次の条件を満足するように取る．

$$(27)\begin{cases} N\mathfrak{g}_1 > k^n, \quad \langle P_\nu^{1/k} \rangle > k \ (\text{十分大}), \quad N\mathfrak{g}_j \cdot P_j > P_{j-1}, \\ P_j \leq c_1(n, j)\, T^{n(1-\frac{1}{k})^j}, \quad P_\nu \geq T^{n(1-\frac{1}{k})^j}, \quad P_0 = T^n \end{cases}$$

そして各 $\mathfrak{g}_j$ は正規化されてあるとし，$\mathfrak{g}_j \parallel \pi_j \in \mathfrak{O}$ としておく，さて我々の定理 6 における λ_i, μ_i に対し

$$(27)\quad \begin{cases} \lambda_i = \varphi_i + \xi_i \pi_1, \quad \mu_i = \psi_i + \eta_i \pi_1 \\ \qquad \varphi_i, \psi_i < c_1 \pi_1 \qquad\qquad (1 \leq i \leq s) \end{cases}$$

とおく，ここで φ_i や ψ_i はそれぞれ mod $\mathfrak{g}_1$ の完全剰余系を動きそれは λ_i や μ_i によって一意に決められるであろう．かくて (25) を書き直すと

$$(28)\ (\varphi_1 + \xi_1 \pi_1)^j + \cdots + (\varphi_s + \xi_s \pi_1)^j = (\psi_1 + \eta_1 \pi_1)^j + \cdots + (\psi_s + \eta_s \pi_1)^j \qquad (1 \leq j \leq k)$$

となる，ここで

$$(29)\qquad \varphi_i + \xi_i \pi_1, \quad \psi_i + \eta_i \pi_1 < T. \qquad (1 \leq i \leq s)$$

とする．

このようにすることが可能であることは代数体の基礎の簡単な性質と素イデアル定理（剰余項などの詳しいことは不用で，例えば [60]）とから容易に出る．

ここで $N_s^{(1)}(P_0)$ を，system $\{\varphi_1, \cdots, \varphi_s\}, \{\psi_1, \cdots, \psi_s\}$ がその中に k 個の異なる φ_i, ψ_i をもつ場合の条件 (29) のもとでの連立方程式 (28) の解の個数を表はすとし，上記の場合に入らないような

$\{\varphi_1,\cdots,\varphi_s\}$, $\{\psi_1,\cdots,\psi_s\}$ に対する上式の前の場合のような解の個数を $N_s^{(2)}(P_0)$ で表はすことにする。このとき次式が分るのである

$$N_s^{(1)} \leqq \binom{s}{k}^2 k!\, c^{k^2 n} P_1^{2k}\, N\delta_1^{\,2s-\frac{1}{2}k(k+1)}\, N_{s-k}(P_1)$$

$$N_s^{(2)} \leqq 2k^s P_1^{2k}\, N\delta_1^{\,s+k-1}\, N_{s-k}(P_1)$$

ここでもし

(30) $$s \geqq \frac{n}{2(n-1)} k(k+1) + k - 1 \quad \left(> \frac{1}{2}k(k+1) + k - 1 \right)$$

とおくならば

先づ, $\binom{s}{k}^2 k! > (s-k+1)^{2k}/k!$ (30)より $> \left(\frac{1}{2}k(k+1)\right)^{2k}/k!$

$$= k^{2k}\left(\frac{k+1}{2}\right)^{2k}/k! = 2k^{2k}\cdot \frac{\left(\frac{k+1}{2}\right)^2}{k} \cdots \frac{\left(\frac{k+1}{2}\right)^2}{2} \cdot \frac{1}{2}\, \frac{\left(\frac{k+1}{2}\right)^2}{1}$$

(31) $$\geqq 2k^{2k}\cdot 1 \cdots 1\cdot 1 = 2k^{2k} \quad (k \geqq 2)$$

($k \geqq 1$ としたいときは $s=2$ とおけばよい)

次に, (30) より

$$-\frac{n-1}{n}s \leqq -\frac{1}{2}k(k+1) - \frac{n-1}{n}(k-1)$$ だから, (27) より

$$k^{s-2k} < N\delta_1^{\frac{s}{n}-\frac{2k}{n}} = N\delta_1^{\,s-\frac{n-1}{n}s-\frac{2k}{n}}$$ これに上式を用いて

$$\leqq N\delta_1^{\,s-\frac{1}{2}k(k+1)-k+1+\frac{k-1}{n}-\frac{2k}{n}} \quad (k \geqq 2)$$

$$< N\delta_1^{\,s-\frac{1}{2}k(k+1)-k+1}$$

かくて, (31) の結果を用いて

$$2k^s N\delta_1^{\,s+k-1} < 2k^{2k} N\delta_1^{\,2s-\frac{1}{2}k(k+1)}$$

$$< \binom{s}{k}^2 k! \, N\mathfrak{f}_1^{\,2s-\frac{1}{2}k(k+1)}$$

$$< \binom{s}{k}^2 k! \, c^{k^2 n} \, N\mathfrak{f}_1^{\,2s-\frac{1}{2}k(k+1)} \qquad (c>1)$$

さて再び(27)からと上式から得る $N_s^{(2)} < N_s^{(1)}$ とから

$$N_s(P_0) \leqq N_s(N\mathfrak{f}_1 P_1) = N_s^{(1)}(P_1) + N_s^{(2)}(P_1) \leqq 2N_s^{(1)}(P_1)$$

$$\leqq 2c^{k^2 n} \binom{s}{k}^2 k! \, P_1^{2k} \, N\mathfrak{f}_1^{\,2s-\frac{1}{2}k(k+1)} \, N_{s-k}(P_1)$$

を得る，これを次のように書き直す

$$(32) \quad \begin{cases} N_s(P) \leqq D_1 \, P^{2k} \, N\mathfrak{f}_1^{\,2s-\frac{1}{2}k(k+1)} \, N_{s-k}(P_1) \\ D_1 = c^{k^2 n} \binom{s}{k}^2 k! \quad (c>2) \end{cases}$$

この操作をつづけて

$$N_s(P) \leqq D_1 D_2 \cdots D_r \, (P_1 P_2 \cdots P_r)^{2k} \, (N\mathfrak{f}_1 N\mathfrak{f}_2 \cdots N\mathfrak{f}_r)^{2s-\frac{1}{2}k(k+1)}$$

$$(33) \qquad \times \, (N\mathfrak{f}_1 N\mathfrak{f}_2^{\,2} \cdots N\mathfrak{f}_r^{\,r-1})^{-2k} \, P_r^{\,2(s-rk)}$$

を得る，ここで実は始めに求めた条件(27)と定数 c, $c_1(n,j)$ 等と先にうまく取っておくと(33)の右辺が求める結果を与えるのである。

実はもし

$$(34) \qquad s \geqq c\,k^2 \log k$$

であるならば

$$(35) \qquad N_{s,k}(T) = \sigma \cdot \mu \cdot T^{(2s-\frac{1}{2}k(k+1))n} + o\left(T^{(2s-\frac{1}{2}k(k+1))n}\right)$$

(ここで σ, μ は Waring 問題の場合に相当するある正の定数である。)が予想されるのであるが未だ言えてない。もっと弱

い結果

(36) $$N_{s,k}(T) \ll T^{(2s - \frac{1}{2}k(k+1))n + \varepsilon} \qquad (\varepsilon > 0)$$

も見当らない. (35) は有理整数解 $\alpha_i, \mu_i, \nu_i \in \mathbb{Z}$ に限れば, すでに Hua によって [50], [51], [10] 与えられている. 又その後の発展もここにある (29), (35), (36) は代数体では $n=1$ の場合よりはるかに多く (n 乗も!) 解をもつことを示している理だが (35), ~~(36)~~ が言える.. 現在では有理整数解以外には存在を論じては出来ないが, Hua の結果 [6], 18 章 §7 の方法を用いると (34) の条件のもとではある程度あることは示しているようである. (35) が言えると §4 の (22)〜(24) は

(37) $$G_K(k) < 2nk\log k + 4nk\log\log k + 2nk\log\log\log k + C(n)k \qquad (k \geqq C)$$

と改良される. (36) でもよいことは最後の所まで見ると分るのであるが [41] 附録にこれに対する注意がある. (定理10).

§6. Vinogradov の平均値定理の応用. (minor arc での三角和の評価について).

定理7. T を十分大きい数とし, 自然数 $k \geqq 2$ とする. $\sqrt{k}\log k < r < k - \sqrt{k}\log k$ とし $\bar{s} = \mathrm{Max}(k-r, r)$, $\underline{s} = s = \mathrm{Min}(k-r, r)$ とする. $f(u) = \alpha_1 u + \alpha_2 u^2 + \cdots + \alpha_{k+1} u^{k+1}$, $\alpha_i = x_{i,1}\rho_1 + \cdots + x_{i,n}\rho_n$, $(x_{i1}, \ldots, x_{in}) \in U$ $(1 \leqq i \leqq k+1)$ とし $\alpha_{k+1} \in \mathcal{E}(h, t)$ とする, ここでは $h = c^n k^s D^2 T^{\bar{s}}$ $(c \geqq 32)$, $t = T^{\underline{s}}$ とする. もし

$$S(\alpha_1, \cdots, \alpha_{k+1}) = \sum_{\lambda < T}' E(\alpha_1 \lambda + \cdots + \alpha_{k+1} \lambda^{k+1})$$

であれば，次の評価を得る：

$$|S| \leqq C\, T^{\, n - \frac{1}{96(\log n + 3)^2 k^2 \log n}}$$

定理 8　定理 1 と同じ条件のもとに今度は $\varepsilon k < r < (1-\varepsilon) k$ $(0 < \varepsilon < 1)$ であれば

$$|S| \leqq c(\varepsilon)\, T^{\, n - \frac{c(\varepsilon, n)}{k^2}}$$

ここで

$$c(\varepsilon, n) = \left\{ 32 \log(2e^2 n) \log(2e^2 n/\varepsilon^2) \right\}^{-1},$$

とする $(e = 2.7182\cdots)$.

定理 9　記述は少し長くなるが結果は p. 24 に更めて定理とした．[55].

T' を自然数として十分大とする．$P = [T'^{1/k}]$，$X_h = [X_0^{\delta^h}]$，$Y_h = [\sqrt{X_h}]$ $(1 \leqq h \leqq s_1)$，ここで $X_0 = [\sqrt{P}]$，$Y_0 = [\sqrt{X_0}]$ とし $s_1 > 2kn$，$\delta = 1 - (s_0/2)/(k - \frac{1}{2})$，$\sigma_h \in \mathfrak{O}$ で $\|\sigma_h\| < Y_h$ $(0 \leqq h \leqq s)$ とし，更に

$$\begin{cases} t = X_0^{1-f} \\ h = X_0^{k-1+f} \end{cases} \quad (0 < f \leqq 1/4), \quad \left(\begin{cases} t_0 = R^b \\ h_0 = R^k t_0^{n-1} \log t_0 \end{cases}, \text{ここで } b = \frac{n}{1+n^2}, \right)$$

$s_0 = [\frac{1}{2} \log k] \leqq \frac{1}{2} \log k$ にとっておく．また

$R = \left[X_0^{1 - \frac{1}{2\sqrt{k}}} \right]$ とする，$\mathcal{E}(t, h)$，$\mathcal{E}(t_0, h_0)$ は夫々 (t, h)，(t_0, h_0) に対する Farey 分解に対する minor arc とする．$n \geqq 2$ とし

$r = 2r_0$, $r_0 > k(k+1)+\tau k$ ($\tau \geq 1$ は自然数とする. $\mathfrak{O} \ni \omega$ は単項イデアル (ω) が素イデアルのとき素数と呼ぶ. 条件

$$\frac{1}{2}cR \leq |\omega^{(p)}| \leq cR, \quad |\arg \omega^{(q)}| \leq \frac{\pi}{4k} \quad \begin{pmatrix} 1 \leq p \leq n \\ n_1+1 \leq q \leq n_1+n_2 \end{pmatrix}$$

であるすべての total positive な素数 ω の全体の集合を $\mathfrak{P}=\mathfrak{P}(R.c)$ で表わす. $\mathfrak{P}$ に入る ω の個数 $\#\mathfrak{P} = P(R,c)$ とおく. 次に

$\mathfrak{Q} = \mathfrak{Q}(s_1, X_0)$ によって

$$\mu = (X_0 + \sigma_1)^k + \cdots + (X_{s_1} + \sigma_{s_1})^k, \quad 0 < |\sigma_i| < Y_i \quad (1 \leq i \leq s_1)$$

の形の $\mathfrak{O}$ の数全体の集合とし $\#\mathfrak{Q} = Q(s_1, X_0)$ とおく. すると

$$Q' = \#\{(\mu, \omega) : \mu \in \mathfrak{Q}(s_1, X_0),\ \omega \in \mathfrak{P}(R.c)\}$$

$$= Q(s_1, X_0)\, P(R.c)$$

を得る. この時

<u>定理</u> $\mathcal{E}(\tau, t) \ni \xi$ とするとき

$$R(\xi) = \sum_{\mu \in \mathfrak{Q}(s_1, X_0)}' \ \sum_{\omega \in \mathfrak{P}(R.c)} E(\mu \omega^k \xi)$$

とおくと

$$R(\xi) \ll Q' X_0^{\rho}$$

$$\rho = \frac{1}{2r_0}\left((k-\tfrac{1}{2})\delta^{s_1} + \tfrac{1}{2}(s_0+1)(1-\tfrac{1}{s_0})^{\tau}(1-\delta^{s_1})(k-\tfrac{1}{2}) - \tfrac{1}{2}\tfrac{b}{n} \right) n$$

を得る. ここで例えば

$$s_1 \geq [\,2k(6+\log(n^2+1))\,],$$

$$\tau \geq [\,\log^2 k + \log k \log\log k + \log k \cdot \log(3n^3)\,] - 1$$

とおくと

$$R(\xi) \ll Q' X_0^{-\frac{b}{8r_0}}$$

となる.

ここで $\ll$-Konst は k, s, K のみに関する定数である.

定理7, 8の証明は Korobov [53] (1958) の方法による. 今後はこれの応用に大いに期待している.

定理9は Vinogradov [17] による. もともと Vinogradov の本[17]によるのだが, それの Körner による応用 [38] を直接用いる.

$$|R(\xi)|^{r_0} \ll R^{(r_0-1)n} V,$$

$$V = V = V(\xi) = \sum_{x} \Delta(x) \sum_{\omega} E(\xi \omega^k x)$$

$x = \mu_1 + \cdots + \mu_n - \mu_1' - \cdots - \mu_{r_1}'$, $\mu, \mu' \in \mathfrak{N}$ の解の個数を $\Delta(x)$ とする.

として, $\xi \in \mathcal{E}(h, t) \cap \mathcal{E}_0(h_0, t_0)$, $\xi \in \mathcal{E}(h, t) \cap (\bigcup_{\gamma} M_{0\gamma})$, ($M_{0\gamma}$ は h_0, t_0 に関する major arc), として二つの場合に分け, V の評価に帰して求める. 尚 p.24 上に代数体での素数の集合 P を用いたが, それに対しての素数定理からの帰結 (というよりはむしろ K での Tschebyschef の定理と呼ぶ方がよいだろう) は Mitsui の素数定理 [57] によれば強力すぎるであろう. この ω の範囲は実は座標軸に平行な直方体で十分な様なので Hecke の (そして Weyl の [17]) 理論 [58] により, 方法は van der Corput [59] による方が簡明であると思う. Fourier analysis 等については最近の Tatuzawa [61] ~ [63] を参照. T を十分大とすれば

$$c_1 \frac{\log T}{T^n} < P(R, C) < c_2 \frac{\log T}{T^n}, \quad c_1, c_2 > 0$$

を得るのである.

§7. 代数体における Waring 問題

今まで Hardy-Littlewood の理論や Siegel, Vinogradov の方法を紹介することに，あはせて述べて来た定理 1,2, 3, 3′, 4, 9 等を用いることによって最後に Waring 問題が次の定理 10 の形に改良されることを示そう．これを更に改良しようとすれば定理 5 が必要になるであろうことも述べた．

定理 10 [55] $k \geqq c$，$n \geqq 2$ であれば

$$G_K(k) < 2n \log k + 6nk \log k$$
$$+ (4n \log n + 2n \log\log n + 12n + 4\log n + 14)k + 1$$

証明．先づ次の記号を用いる．

$\epsilon \succ 0$ 単数，$J_k \ni \nu \succ 0$，$N(\nu) \geqq C$．$\nu_0 = \epsilon^k \nu$，$A = \sqrt[n]{N(\nu)}$

実共軛を l，複素共軛を m で示して，$0 < c_1 < c_2$ に対して

$$c_1 A/\Delta^{2n_2} < \nu_0^{(l)} < c_2 A/\Delta^{2n_2}, \quad c_1 \Delta^{n_1} A < |\nu_0^{(m)}| < c_2 \Delta^{n_1} A \quad (0 < \Delta < \tfrac{1}{2})$$

となるように Δ に無関係に $c_1, c_2 > 0$ がとれる．$s = 2s_0 = 2[\log k]$，$s_1 = [2k(6 + \log(n^2+1))]$，$s_2 = n[k(\log k + 3\log\log k + 2\log n + \log\log n + 4)]$，$a = 1/k$．$T = (c_2 A/\Delta^{2n_2})^a$，$T' = c_2 A/\Delta^{2n_2}$，$\tilde{T} = (c_1 \Delta^{n_1} A/(4s_2 + 2(2c_3)^k s_1))^a$．$X_0 = [\sqrt{P}]$．$[\tilde{T}] = P$．$\tau = \nu_0 - \sigma_1 - \sigma_2 - \mu\omega^k$，$\sigma_1, \sigma_2 \in \mathfrak{G}_0(s_2, \tilde{T})$，$\omega \in \mathfrak{R}(R, c_3)$，$R = X_0^{1 - \frac{1}{2\sqrt{k}}}$，$\mu \in \mathfrak{G}(s_1, X_0)$ に対し

$$c_1 A/2\Delta^{2n_2} < \tau^{(l)} < c_2 A/\Delta^{2n_2}, \quad c_1 \Delta^{n} A/2 < |\tau^{(m)}| < (c_2 + \tfrac{1}{2}c_1)\Delta^{n_1} A$$

を得る．

$L = X_0^{k-1+\delta}$, $t = X_0^{1-\delta}$, $\delta = \frac{1}{4}$. によって Farey 分割を行う.

次の三角和を定義する.

$$\begin{cases} L(\xi) = \sum_{\lambda < T} E(\lambda^k \xi), \qquad V(\xi) = \sum_{\sigma \in Q_0(s_2, \tilde{T})} E(\sigma \xi) \\ R(\xi) = \sum_{\mu \in Q(s_1, X_0)} \sum_{\omega \in R(R, c_3)} E(\mu \omega^k \xi) \end{cases} ; \quad s_1 > 4nk \text{ にとる.}$$

かくて Farey 分割によって

$$\sum_{\gamma \in \Gamma} \int_{m_\gamma} L^{4nk+1}(\xi) V^2(\xi) R(\xi) E(-\nu\epsilon^k \xi)\, dx \quad \text{を作ると}$$

$$= \sum_{\tau = \nu_0 - \sigma_1 - \sigma_2 - \mu\omega^k} \sum_{\gamma} \int_{m_\gamma} L^{4nk+1}(\xi) E(-\tau\xi)\, dx, \quad \nu_0 = \nu\epsilon^k, \quad s = 4nk+1$$

ここで $\tau / T^k = \mu$ とおくと $0 < c_1/2c_2 < \mu^{(1)} < 1$, $|\mu^{(n)}| < 1$ つまり $\mu < 1$ を得る. ここで定理 1, 2 から 上式は (追記参照)

$$= \sum_{\tau} \left(\sigma J \cdot T^{n(s-k)} + O\left(T^{n(s-k) - \frac{1}{4}}\right) \right)$$ を得る. Δ を十分小に取ると定理 3, 3′ と p. の定理 11 とから $J > c > 0$ $(\Delta \to 0)$.

以上から

$$(37) \quad \mathrm{Re} \sum_{\gamma} \int_{m_\gamma} L(\xi)^{4nk+1} V^2(\xi) R(\xi) E(-\nu\epsilon^k \xi)\, dx > c Q_0^2(s_1 \tilde{T}) Q' T^{(s-k)n}, \quad c > 0$$

次に minor arc では定理 4, 9 によって

$$\int_{E} L(\xi)^{4nk+1} V^2(\xi) R(\xi) E(-\nu\epsilon^k \xi)\, dx \ll \sup_{\xi \in E} \left| L(\xi)^{4nk+1} R(\xi) \right| \int_{U} |V(\xi)|^2 dx$$

$$\ll T^{sn} Q_0(s_2, \tilde{T}) Q' X_0^{\rho} \cdot Q_0(s_2 \tilde{T}) \tilde{T}^{-nk + nk(1-\frac{1}{k})^{\ell}}$$

$$= T^{(s-k)n} \cdot Q_0^2(s_2, \tilde{T}) Q' X_0^{\rho + nk(1-\frac{1}{k})^{\ell}}, \quad \ell = \left[\frac{s_2}{n}\right].$$

かくて

$$(38) \quad \ll Q_0^2(s_2, \tilde{T}) Q' T^{(s-k)n} X_0^{\sigma}$$

ここで定理9によれば，次のように $s_1,\ s_2$ を取れば $\sigma < -c$

$c > 0$ がいえる．かくて (37), (38) から

$$\int_U L^s(\xi)\, V^2(\xi)\, R(\xi)\, E(-\nu\epsilon^k \xi)\, dx > 0$$

がいえることになる．このことは

$$\nu\epsilon^k = \sum_{j=1}^{s} \lambda_j^k + \sum_{j=1}^{2s_2} \sigma_j + \sum_{j=1}^{s_1} \tau_j$$

と表わされるような total non-negative な $\lambda_j,\ \sigma_j,\ \tau_j \in \mathfrak{O}\ (\in J_k)$

が存在することを示しているし，ここに

$$\begin{cases} N(\lambda_j) \le T^n = c\,N(\nu)^{1/k}, & N(\sigma_j) \le \tilde{T}^k < c\,N(\nu)^{1/k} \\ N(\tau_j) \le X_0^n R^n = c\,N(\nu)^{1/k} & \end{cases}$$

であること，および

$$\begin{aligned} G_K(k) &\le s + s_1 + 2s_2 \\ &\le (4nk+1) + \Big(2k(6 + \log(n^2+1)) \\ &\qquad + 2nk\,(\log k + 3\log\log k + 2\log n + \log\log n + 4) \Big) \\ &\le 2nk\log k + 6nk\log\log k \\ &\qquad + 2(2n\log n + n\log\log n + 6n + 4\log n + 14)k + 1 \end{aligned}$$

であることは明かである．

（以上）

追記. i) P.11 の下に続いて次の定理を入れる：

定理 2′ $\nu > 0$, $s \ge \frac{1}{f} nk + 1$ $(0 < f \le \frac{1}{4})$, $\mu = T^{-k}\nu$, $\nu < T^k$

ならば

$$\sum_{\gamma} \int_{\mathfrak{M}_\gamma} f(x)^s E(-\nu\xi)\, dx = \sigma J(\mu) T^{n(s-k)} + O(T^{n(s-k)-f}).$$

ii) 定理6は[49]の原文がミスプリントが多いので s についての部分を丁寧に記しておいた。(iii) [1] は未見であるが Waring 問題の始まりであるので Hilbert や Hardy によって記した。(iv) 以下に目次をあげておく

目次

文　　献

[1] E. Waring: Meditationes Algebraicae, ed. 3 (1782), 349-350.

[2] D. Hilbert: Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl nter Potenzen (Waringsche Problem), Göttinger Nachrichten, (1909), 17-36, (Math. Ann. Vol. 67 (1908), 281-300).

[3] E. Landau: Vorlesungen über Zahlentheorie, 1, Verlag von S. Hirzel, Leipzig, (1927).

[4] " " : Über einige neuere Fortschritte der additiven Zahlentheorie, Cambridge, (1937).

[5] 池原止戈夫： 初等解析的整数論, 河出書房 (1949).

[6] 華羅庚 ： 数論導引, 科学出版社, 北京 (1957).

[7] G.H. Hardy - E. Wright: An introduction to the theory of numbers, ed. 3, Oxford, (1960).

[8] R. Ayoub: An introduction to the analytic theory of numbers. Amer. Math. Soc. Math. Surveys, (1963).

[9] I.M. Vinogradov: The method of trigonometrical sums in the theory of numbers, (K.F. Roth - A. Davenport による英訳), Interscience Publishers, (1954).

[10] L.K. Hau: Additive theory of prime numbers, Trans. Math. Monograph. 13, Amer. Math. Soc. (1965) (初版はロシア語(1941), 改訂版 堆壘素数論 (1953) 北京, 修訂本(1957) 北京, 英訳はこれによる. 独訳もあり).

[11] H. Davenport: Analytic methods for Diophantine equations and Diophantine inequalities, Campus Publiohers, Michigan, (1963).

[12] G.H. Hardy: Some famous problems of the theory of numbers and in particular Waring's problem. An inaugural lecture delivered before the University of Oxford, Oxford, (1920), pp. 34.

[13] P. Barrucand: Le problème de Waring et la méthode de Hardy [Dissection de Hardy]. Séminaire Delange-Pisot, (Théorie des nombres) 3e année, 15 (1961/62), 1-34.

[14] G.H. Hardy: Collected papers of G.H. Hardy. Vol. 1, Oxford, (1966).

[15] И.М.Виноградов (I.M. Vinogradov): Избранные Труды, Изд. АН СССР, (1952).

[16] G.H. Hardy - S. Ramanujan: Asymptotic formulae in combinatory analysis. Proc. London Math. Soc. (2). 17 (1918), 75-115.

[17] H. Weyl: Über die Gleichverteilung von Zahlen mod Eins. Math. Ann. 77 (1916), 213-352.

[18] G.H. Hardy - J.E. Littlewood: A new solution of Waring's Problem. Quat. J. 48 (1920), 272- 93.

[19] G.H. Hardy - J.E. Littlewood: Some problem of 'Partitio Numerorum' ; I : A new solution of Waring's Problem. Nachr. Göttingen, 5 (1920), 33-54.

[20] " " : P.N. II. Proof that every large number is the sum of at most 21 biquadrates. Math. Zeit. 9 (1921), 14-27.

[21] " " : P.N. IV. The singular series in Waring's Problem and the value of the number $G(k)$。 Math. Zeit. 12 (1922), 161-188.

[22] " " : P.N. VI. Further researches in Waring's Problem. Math. Zeit. 23 (1925), 1-37.

[23] " " : P.N. VIII. The number $\Gamma(k)$ in Waring's Problem. Proc. London Math. Soc. (2), 28 (1928), 518- 42.

[24] И.М. Виноградов: Новая оценка $G(n)$ в проблеме Варинга. Доклады Ak. Hayk. СССР. 4 (1934), 181-187.

[25] " " : О верхней границе $G(n)$ в проблеме Варинга, ИАН. СССР. 10 (1934), 1455-1469.

[26] " " : On Waring's problem. Ann. Math. 36 (1935), 395-405.

[27] " " : К вопросу о верхней границе для $G(n)$, ИАН. СССР. 23 (1959), 637-642.

[28] C.L. Siegel: Darstellung total positiver Zahlen durch Quadrate Math. Zeit. 11 (1921), 246-275.

[29] " " : Additive Theorie der Zahlkörper I. Math. Ann. 87 (1922), 1-35.

[30] " " : " " " II. Math. Ann. 88 (1923), 184-210.

[31] " " : Generalization of Waring's Problem to algebraic number field. Amer. J. Math. 66 (1944), 122-136.

[32] " " : Sums of m^{th} powers of algebraic integers. Ann. Math. 46 (1945), 313-339.

[33] T. Tatuzawa: On the Waring problem in an algebraic number field. J. Math. Soc. Japan, 10 (1958), 322-341.

[34] S.I. Borewicz - I.R. Šafarevič: Zahlentheorie, Birkhäuser Verlag. 1966 (原本ロシア語 他に 佛訳, 英訳あるも独訳よく, 英訳は ミスプリント 多し).

[35] C.P.Ramanujan : Sums of m-th powers in p-adic rings. Mathematik, 10 (1963), 137-146.

[36] T. Tatuzawa: Supplement, Corrections and refinements (1962).

[37] " " : On the Siegel theory concerning the Waring problem in an algebraic number field. (未刊) (1962).

[38] O. Körner: Über das Waringsche Problem in algebraischen Zahlkörper. Math. Ann. 144 (1961), 224-238.

[39] R.M. Stemmer: The easier Waring problem in algebraic number fields. Acta Arith. 6 (1961), 447-468.

[40] L.K. Hua: Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie, Enz. Math. Wiss., I 2, (13), Teil I. 1959.

[41] " " : 指数和的估計及其在数論中的応用, 科学出版社, 北京 (1963). ([40] の改訂版).

[42] " " : An improvement of Vinogradov's mean-value theorem and several applications, Quart. Journ. Math. 20 (1949), 48-61.

[43] A. Walfisz: Weylsche Exponentialsummen in der neueren Zahlentheorie, Math. Forschungsberichte, Veb. Deutscher Verlag der Wiss. Berlin, 1963.

[44] A.A. Карацуба - Н.М. Коробов: О теореме о среднем доказы Akad. Hayk СССР. 149 (1963), 245-248. (Sov. Math. 4, 250-254; On the mean-value theorem).

[45] 竜沢周雄: 或種不定方程式の解について, 1959年5月.

[46] O. Körner: Über Mittelwerte trigonometrischer Summen und ihre Anwendung in algebraischen Zahlkörpern. Math. Ann. 147 (1962), 205-239.

[47] L.K. Hua: On a generalized Waring problem. Proc. London Math. Soc. (2) 43 (1937), 161-182.

[48] R.G. Ayoub: On the Waring-Siegel theorem. Canad. J. Math. 5 (1953), 439-450.

[49] Y. Eda: On the mean-value theorem in an algebraic number field. Jap. J. Math. 36 (1967), 5-21.

[50] 華羅庚: 等幂和問題解数的研究, 数学学報 2 (1952), 65-130.

[51] L.K. Hua: On the number of solutions of Tarry's problem. Acta Sci. Sinica. 1 (1952), 1-76.

[52] Y. Eda - T. Kitayama: Note on the generalized Prouhet-Tarry problem in an algebraic number field. Sci. Rep. Kanazawa, 14 (1969), 21-28.

[53] Н.М. Коробов: Оценки сумм Вейля и распределение простых чисел, Док. Akad. Hayk. СССР. 123 (1958), 28-31.

[54] Y. Eda: On some estimations of the trigonometrical sums in an algebraic number field. (未刊)

[55] (未刊)

[56] M.J. Greenberg: Lectures on Forms in many variables, Benjamin (1969).

[57] T. Mitsui: Generalized prime number theorem. Jap. J. Math. 26 (1956), 1-42.

[58] E. Hecke: Eine neue Art von Zetafunktionen und ihre Beziehung zur Verteilung der Primzahlen II, Math. Zeit. 6 (1920), 11-51.

[59] J.G.v.d. Corput: Diophantische Ungleichungen I, Zur Gleichverteilung Modulo Eins. Acta Math. 56 (1931), 373-456.

[60] Y. Eda, N. Nakagoshi: An elementary proof of the prime ideal theorem with remainder term, Kanazawa Sci. Rep. 12 (1967), 1-12.

[61] T. Tatuzawa: Some results in the Fourier analysis, Nagoya Math. J. 27 (1966), 55-59.

[62] " " : Some remarks in the Fourier analysis, Nagoya Math. J. 29 (1967), 217-219.

[63] " " : On the Fourier Series and Integrals of the Function with Many Variables, Sci. Papers. College. General Education Univ. Tokyo, 19 (1969), 25-33.

[64] T. Mitsui: On the Goldbach problem in an algebraic number field I, J. Math. Soc. Japan 12 (1960) 290-324.